CLAIMS

1. A processing apparatus of secret information constructed by an arithmetic operation processing circuit, a storing circuit, and a signal line connecting them,

in which said processing apparatus of the secret information is constructed so as to obtain a same processing result as a processing result obtained by processing the secret information and data as a processing target by a well-known processing method,

wherein said storing circuit holds

secret information forming information different from said secret information and

secret information forming information processing means for outputting said processing result by using said secret information forming information and said data serving as a processing target without allowing said secret information to appear in said arithmetic operation processing circuit, said storing circuit, and said signal line, and

said arithmetic operation processing circuit executes said secret information forming information processing means.

2. An apparatus according to claim 1, wherein said storing circuit holds said secret information forming information as a plurality of secret information partial information.

Sub A1

3. An apparatus according to claim 1 or 2, wherein said storing circuit further has converting means for converting said secret information forming information into another secret information forming information, and

said another secret information forming information is information for allowing said secret information forming information processing means to output the same processing result as said processing result.

4. An apparatus according to any one of claims 1 to 3, wherein said secret information is a private key for decrypting or forming a digital signature in a public key encryption technique.

5. An apparatus according to any one of claims 1 to 4, wherein said arithmetic operation processing circuit executes said converting means at a predetermined timing.

6. A processing program of secret information in a processing apparatus constructed by an arithmetic operation processing circuit, a storing circuit, and a signal line connecting them,

in which said processing program of the secret information is constructed so as to obtain a same processing result as a processing result obtained by processing the secret information and data as a processing target by a well-known processing method,

wherein said arithmetic operation processing circuit is allowed to output said processing result

by using secret information forming information different from said secret information and said data serving as a processing target

without allowing said secret information to appear in said arithmetic operation processing circuit, said storing circuit, and said signal line.

7. A program according to claim 6, wherein said processing program of secret information processes a plurality of secret information partial information as said secret information forming information.

Sub A7

8. A program according to claim 6 or 7, further comprising converting means for converting said secret information forming information into another secret information forming information,

and wherein said processing program of secret information outputs the same processing result as said processing result by using said another secret information forming information.

9. A processing system of secret information for transmitting and receiving the processing result by using said secret information by using a processing apparatus of secret information according to any one of claims 1 to 5,

wherein an apparatus on a receiver side of said processing result has means for setting said secret information forming information processing means and said secret information forming information into said storing circuit of said processing apparatus,

and an apparatus on a user side of the processing apparatus comprises means for inputting the data serving as a processing target to said processing apparatus, means for receiving said processing result from said processing apparatus, and means for transmitting said received processing result to said receiver side apparatus.